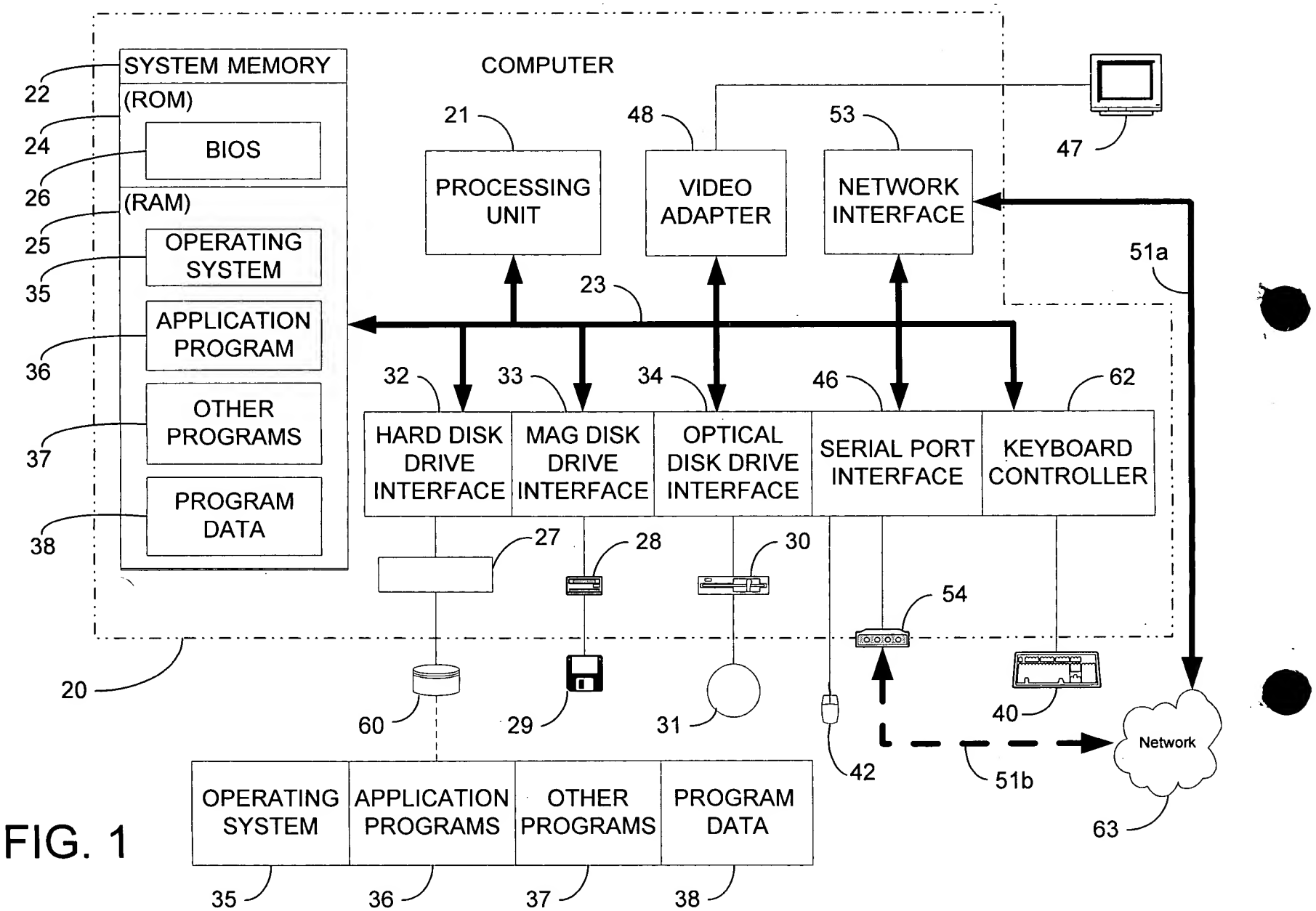
SYSTEM MEMORY
(ROM)
BIOS
(RAM)
OPERATING SYSTEM
APPLICATION PROGRAM
OTHER PROGRAMS
PROGRAM DATA
COMPUTER
PROCESSING UNIT
VIDEO ADAPTER
NETWORK INTERFACE
HARD DISK DRIVE INTERFACE
MAG DISK DRIVE INTERFACE
OPTICAL DISK DRIVE INTERFACE
SERIAL PORT INTERFACE
KEYBOARD CONTROLLER
Network
OPERATING SYSTEM
APPLICATION PROGRAMS
OTHER PROGRAMS
PROGRAM DATA
22
24
26
25
35
36
37
38
21
48
53
47
23
51a
32
33
34
46
62
27
28
30
54
20
60
29
31
40
42
51b
63
35
36
37
38

FIG. 1

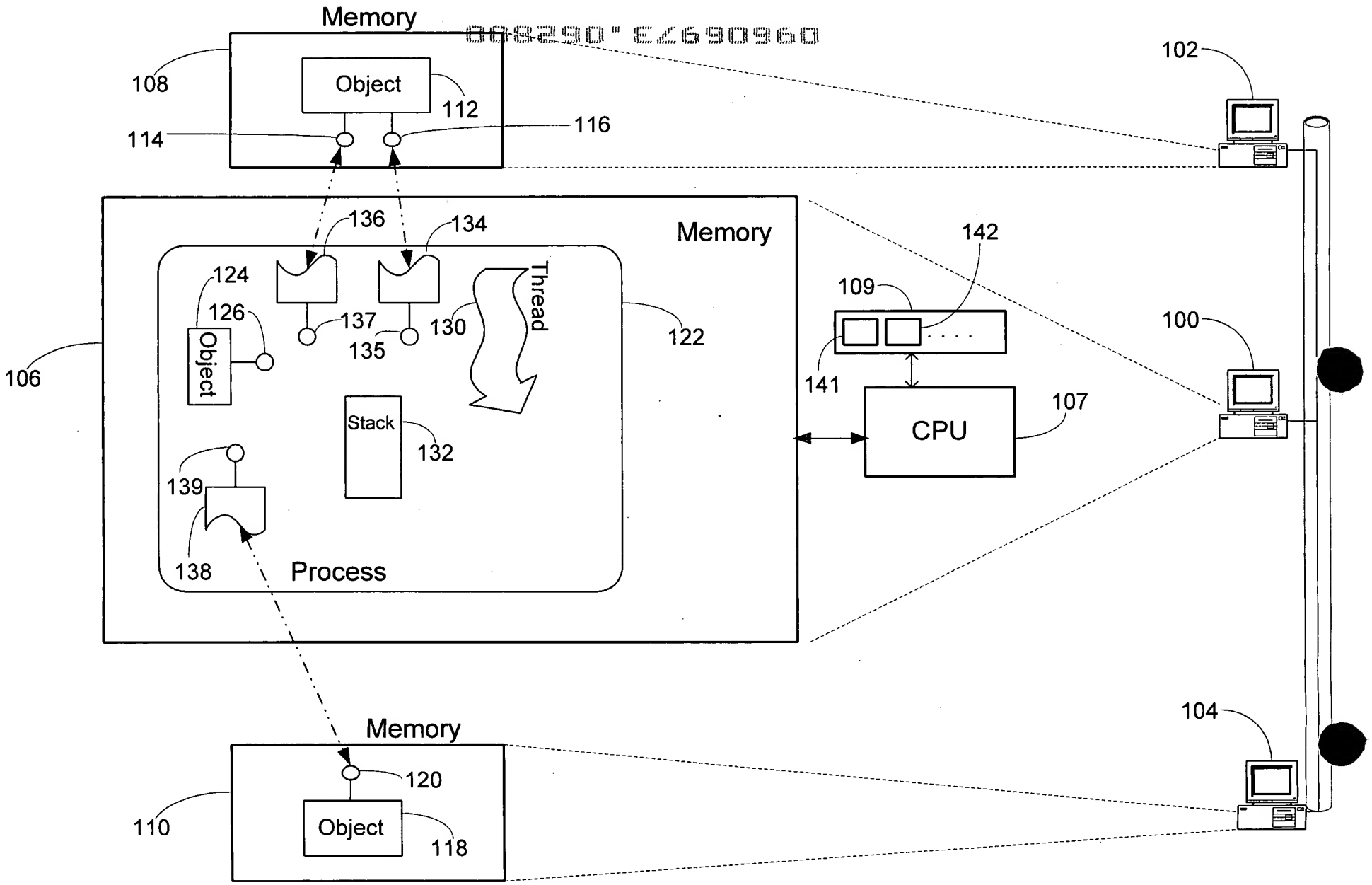
Memory
Object
108
112
114
116
102
136
134
Memory
142
124
126
Object
137
135
130
Thread
109
122
106
100
141
Stack
132
CPU
107
139
138
Process
104
Memory
120
110
Object
118

FIG. 2

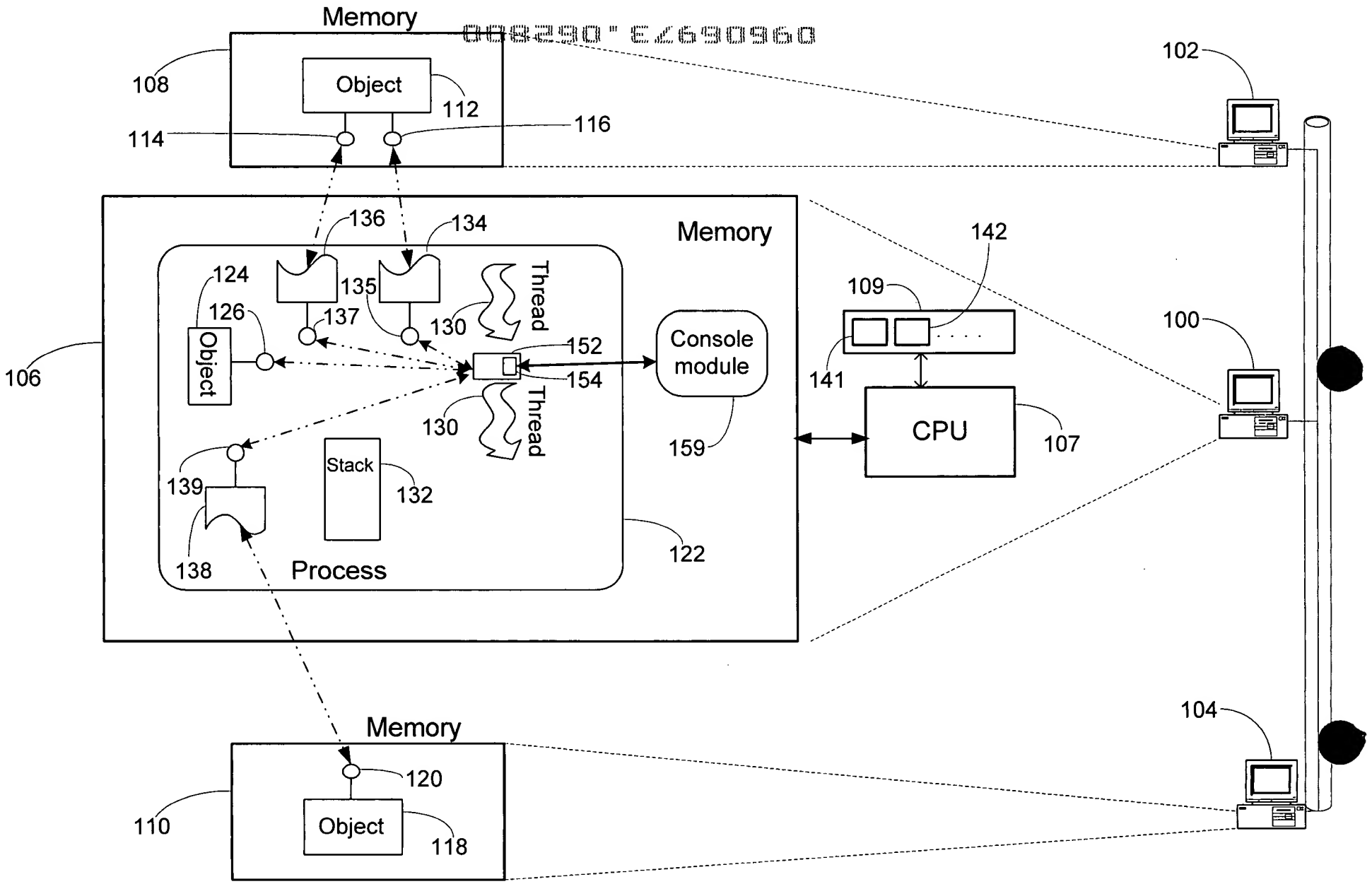
Memory
Object
108
112
114
116
102
Memory
136
134
124
135
Thread
126
137
130
152
Object
106
154
Console module
142
109
141
100
130
Thread
159
CPU
107
Stack
139
132
138
Process
122
Memory
104
120
110
Object
118

FIG. 3

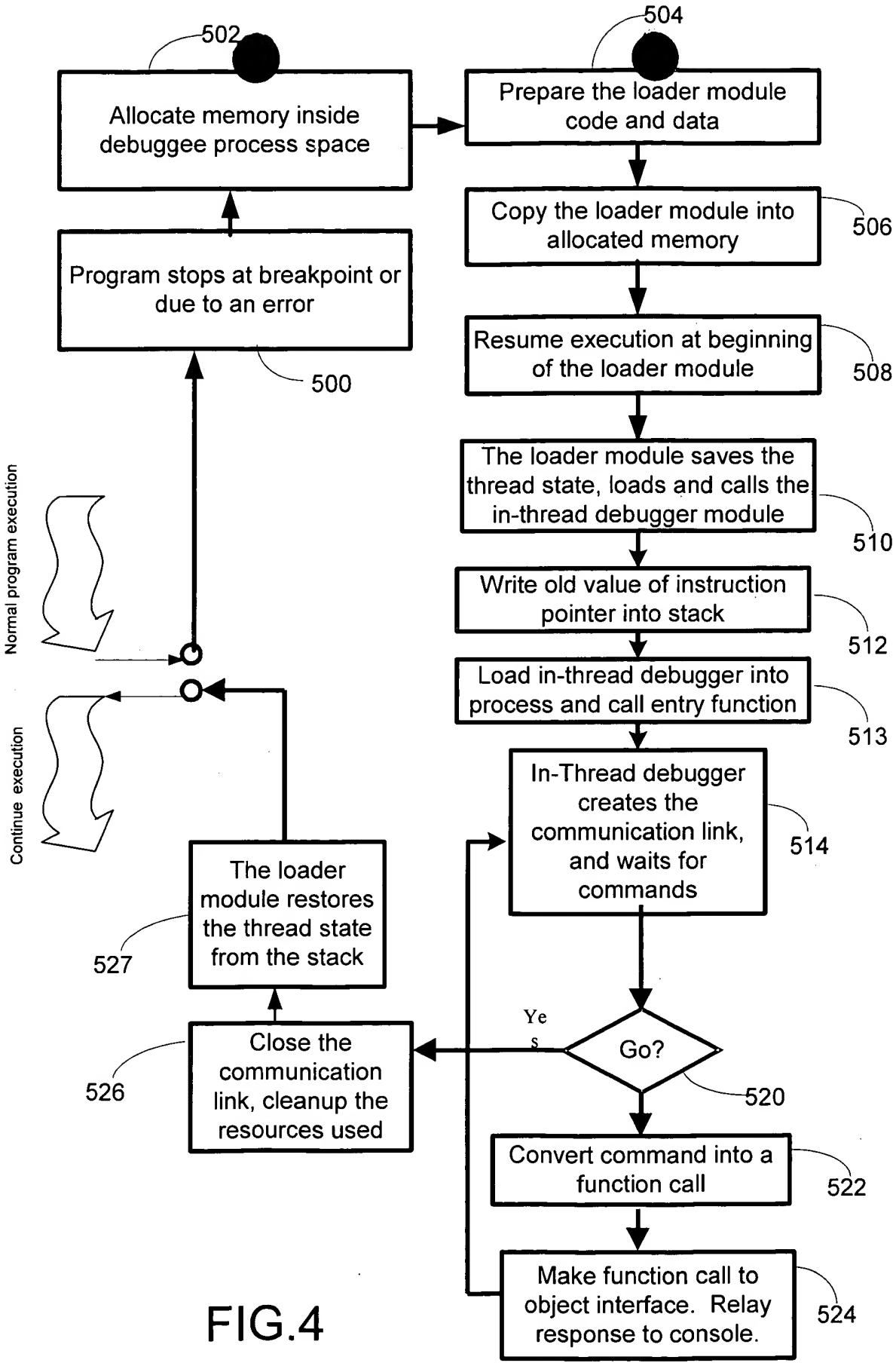
502
Allocate memory inside debuggee process space
504
Prepare the loader module code and data
Copy the loader module into allocated memory
506
Resume execution at beginning of the loader module
508
The loader module saves the thread state, loads and calls the in-thread debugger module
510
Write old value of instruction pointer into stack
512
Load in-thread debugger into process and call entry function
513
In-Thread debugger creates the communication link, and waits for commands
514
Go?
Yes
520
Convert command into a function call
522
Make function call to object interface. Relay response to console.
524
Close the communication link, cleanup the resources used
526
The loader module restores the thread state from the stack
527
Program stops at breakpoint or due to an error
500
Normal program execution
Continue execution

FIG.4

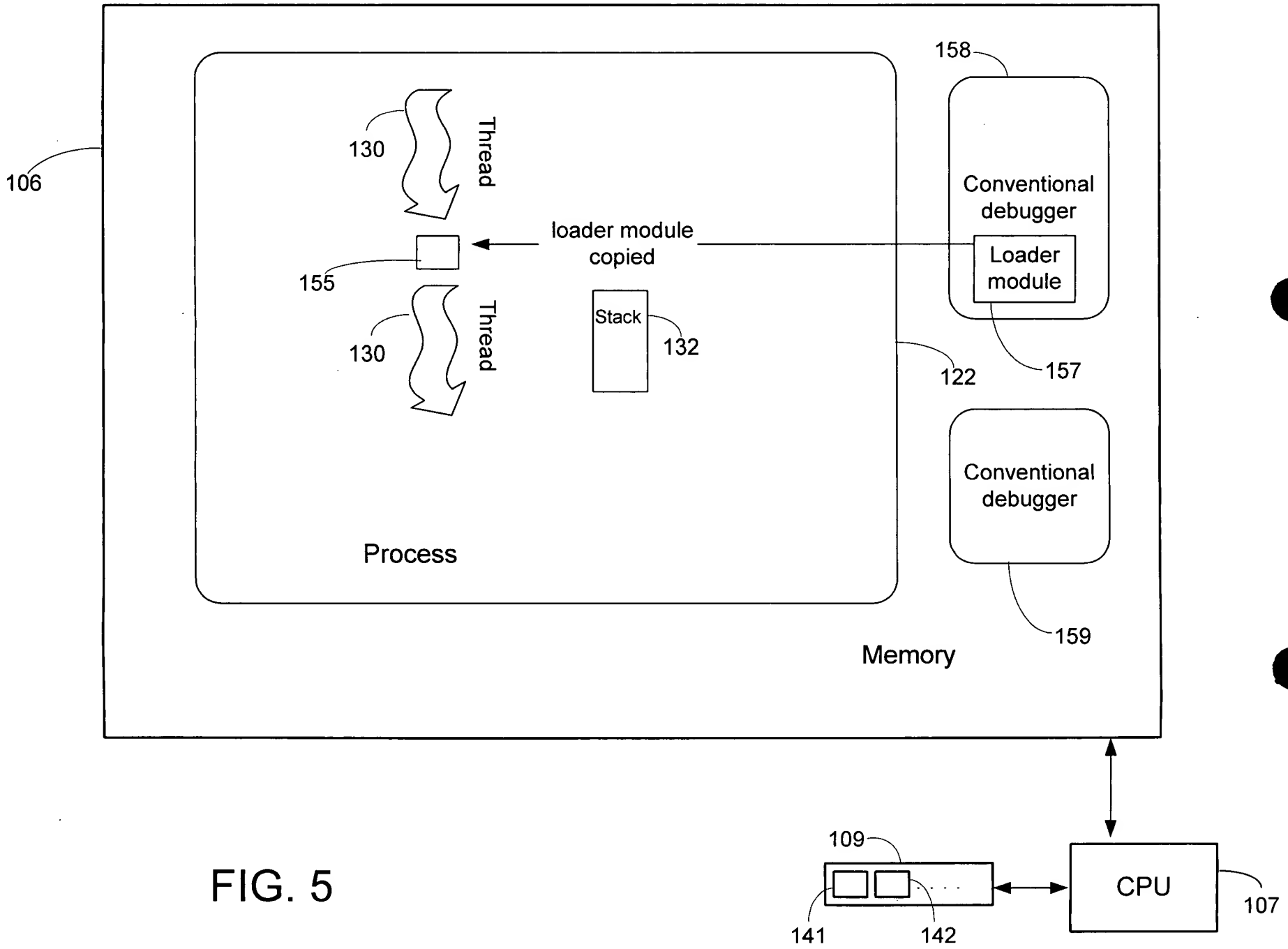
106
130
Thread
155
loader module
copied
130
Thread
Stack
132
Process
158
Conventional
debugger
Loader
module
157
122
Conventional
debugger
159
Memory
109
141
142
CPU
107

FIG. 5

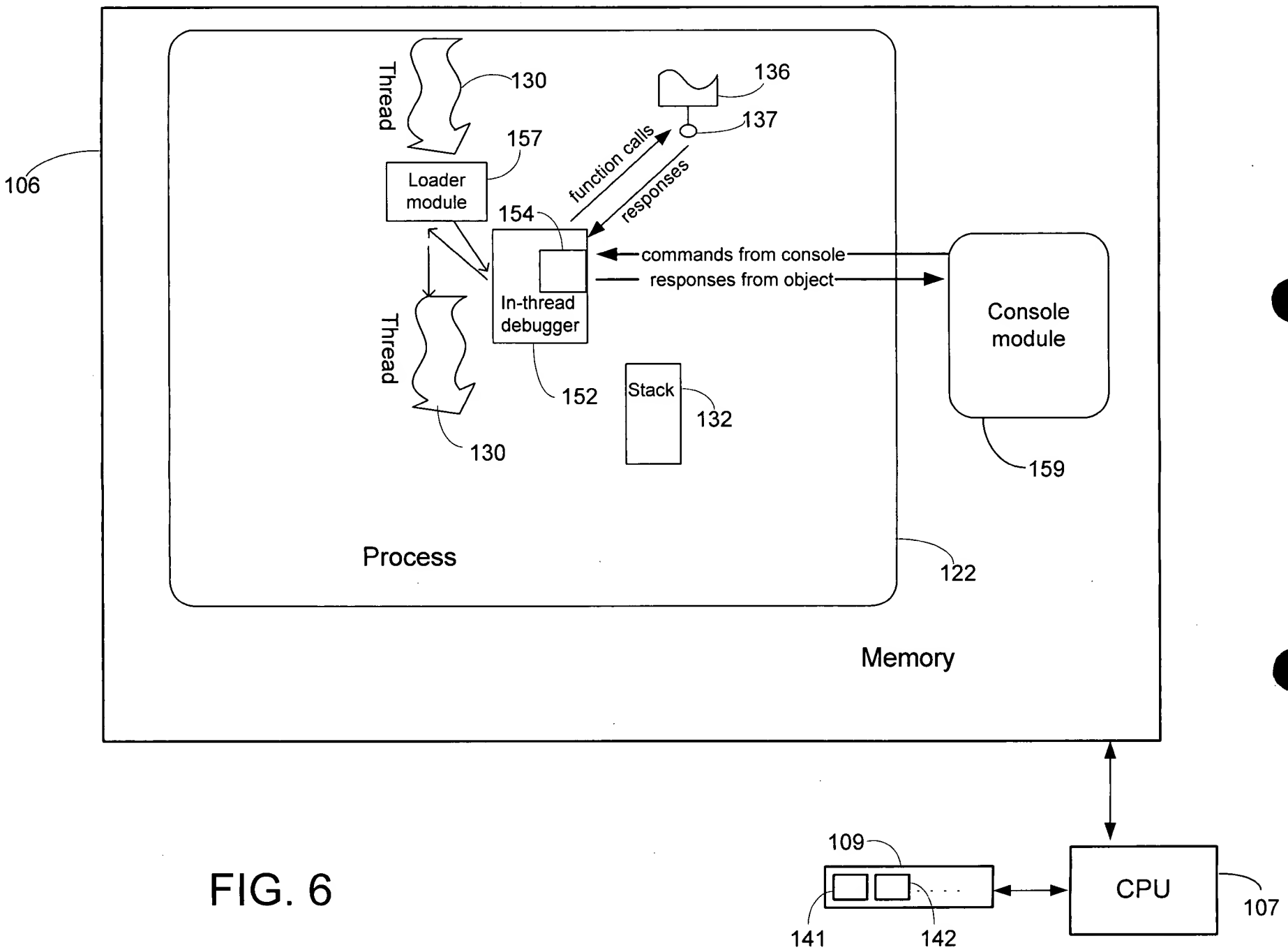
106
Thread
130
136
137
157
Loader module
function calls
responses
154
commands from console
responses from object
In-thread debugger
Thread
152
Stack
132
130
Console module
159
Process
122
Memory
109
CPU
107
141
142

FIG. 6

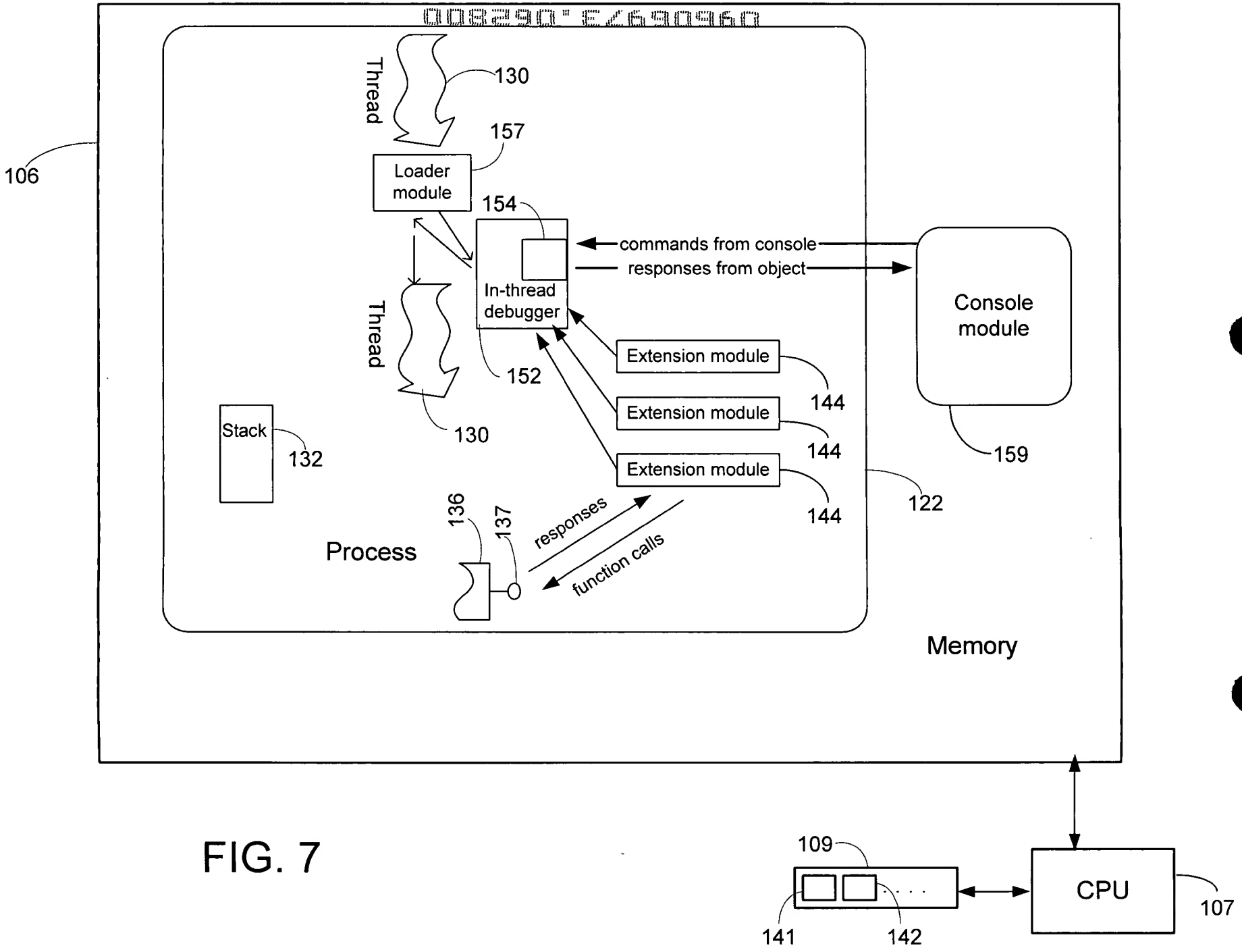
106
Thread
130
157
Loader module
154
In-thread debugger
commands from console
responses from object
Console module
159
Thread
130
152
Extension module
144
Extension module
144
Extension module
144
122
Stack
132
136
137
responses
function calls
Process
Memory
109
CPU
107
141
142

FIG. 7

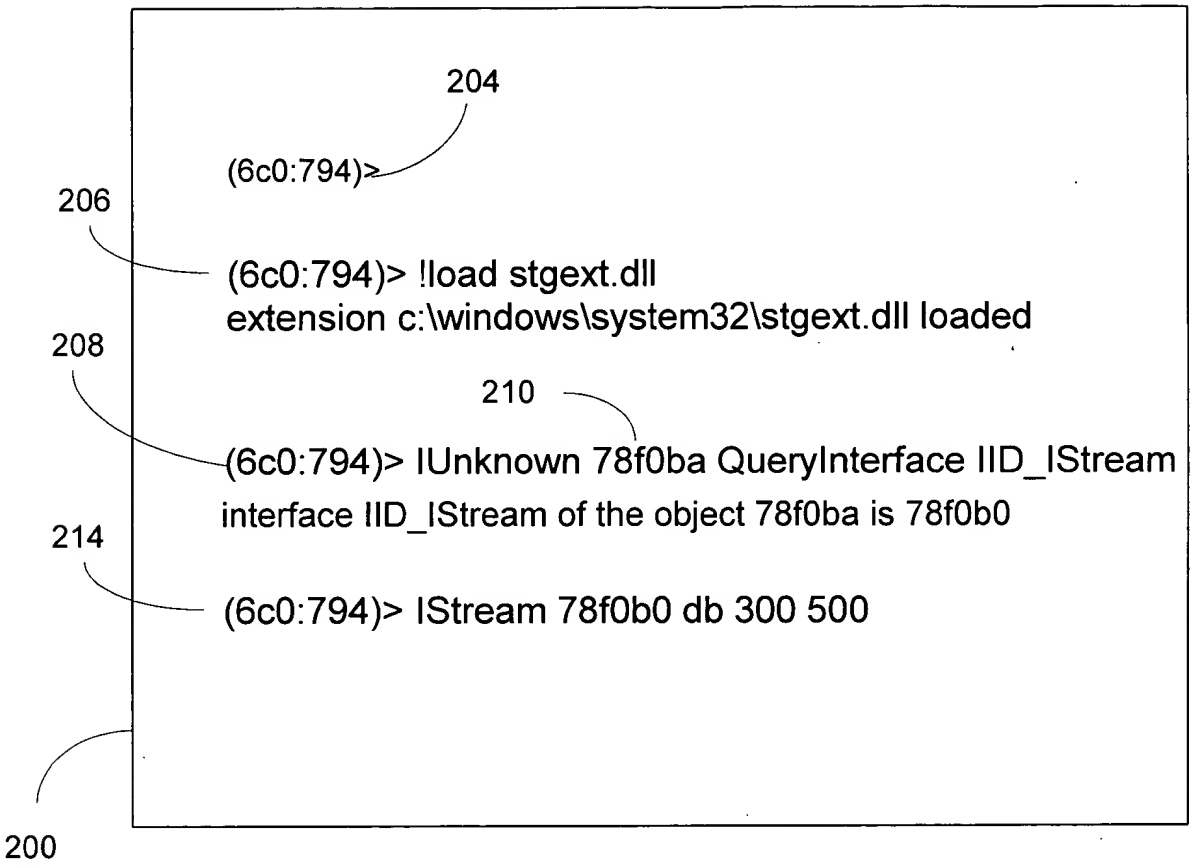
204
(6c0:794)>
206
(6c0:794)> !load stgext.dll
extension c:\windows\system32\stgext.dll loaded
208
210
(6c0:794)> IUnknown 78f0ba QueryInterface IID_IStream
interface IID_IStream of the object 78f0ba is 78f0b0
214
(6c0:794)> IStream 78f0b0 db 300 500
200

FIG. 8

DOCKET: 5050.0002

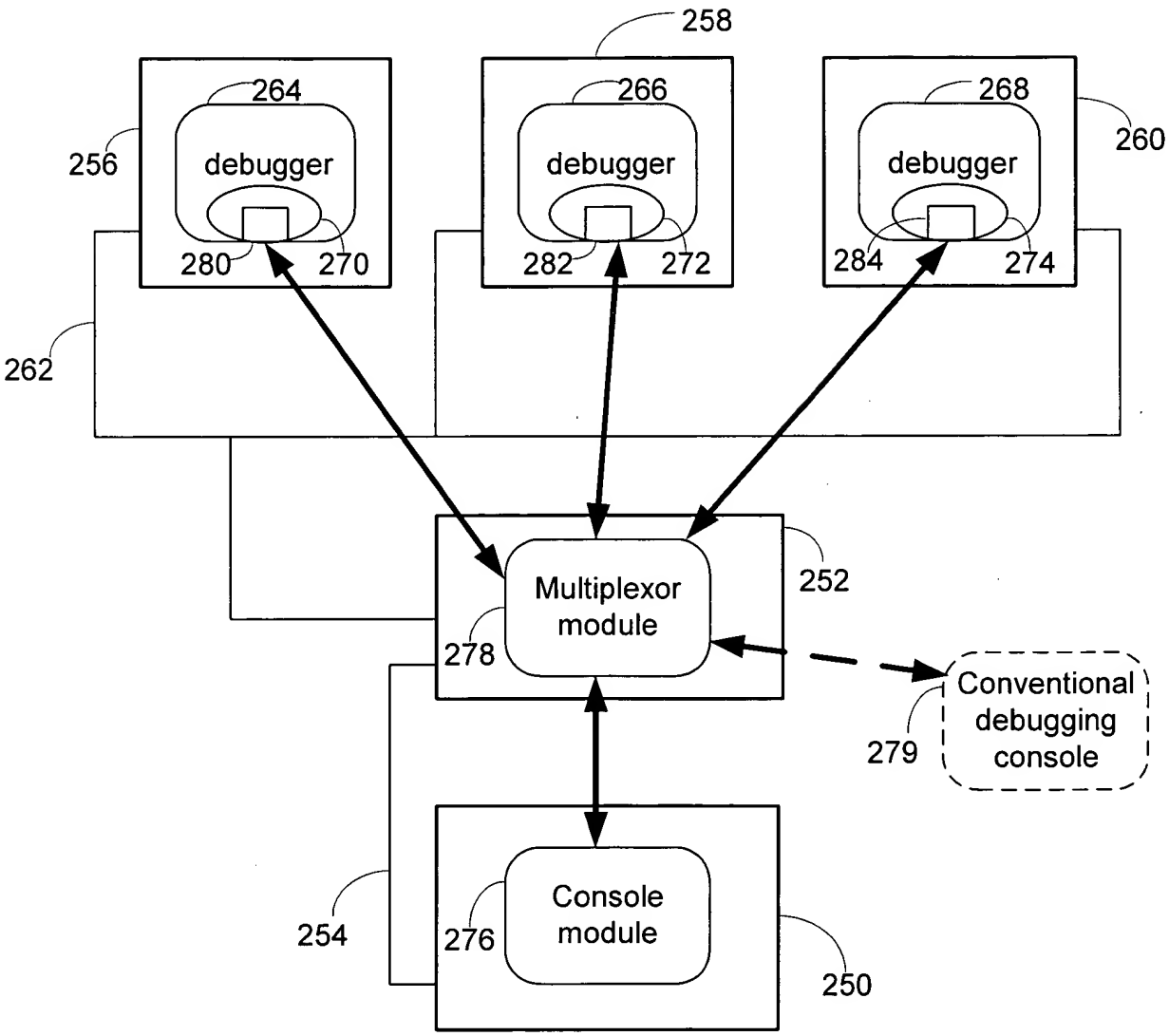

FIG. 9

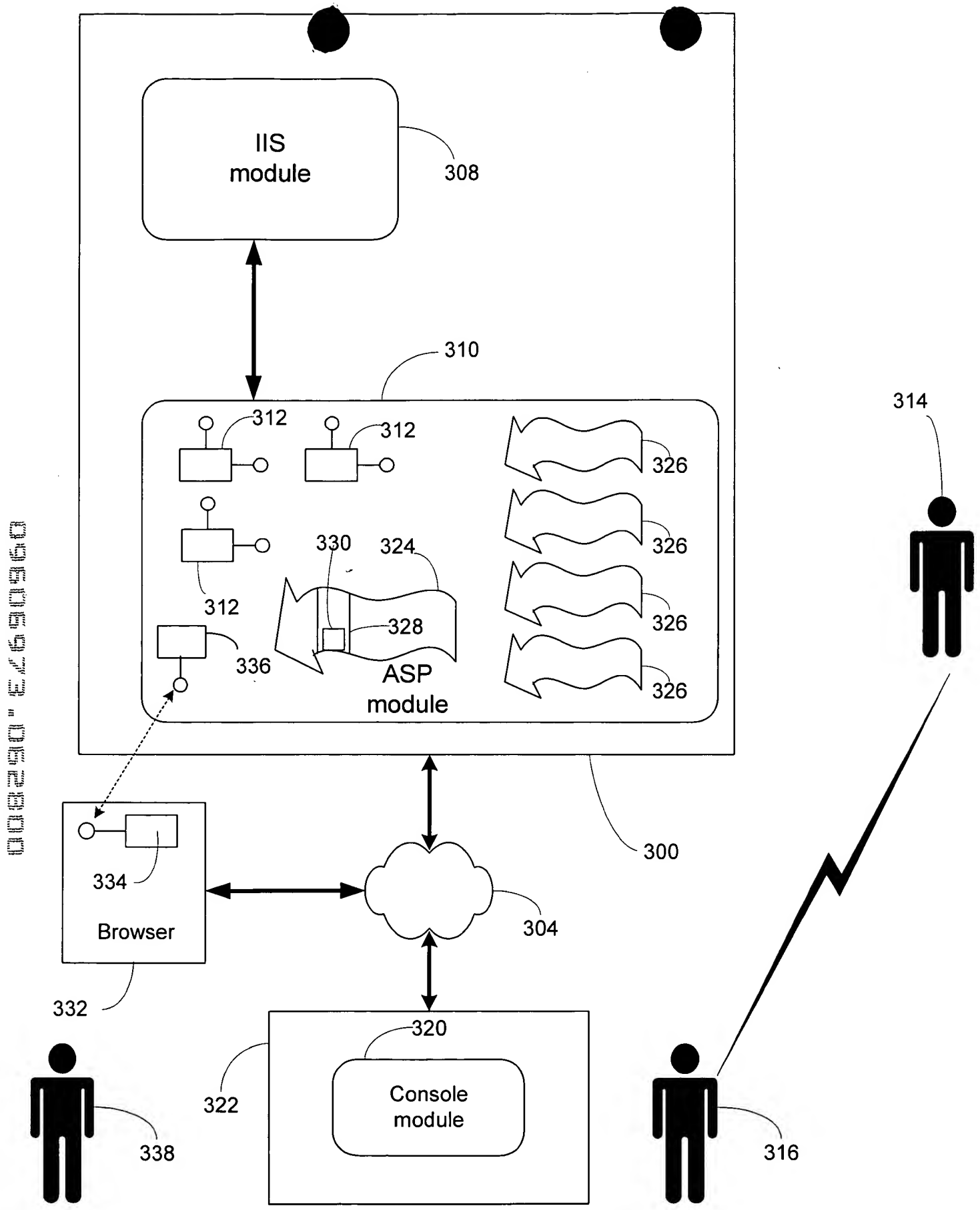
IIS
module
308
310
312
312
312
326
326
326
326
330
324
328
336
ASP
module
314
334
Browser
332
304
300
320
Console
module
322
338
316

FIG. 10